IMPLEMENTATION PLAN FOR DEMONSTRATING JMCIS ON-LINE SERVICES AT CINCPACFLT AND SELECTED PACIFIC FLEET SHIP(S)

(Short Title: JMCIS On-line Services Demonstration Plan)
(JOSDEP)

29 February 1996

NCCOSC RDT&E DIV
San Diego, CA 92152-5001

Do not distribute to DTIC or other data depositories.

Distribution authorized to DoD components only; premature distribution 2/29/96.
Other requests shall be referred to Commanding Officer,
Naval Command, Control and Ocean Surveillance Center (NCCOSC)
RDT&E Division (NRaD)
San Diego, CA 92152-5000

Project Manager:

Mike Kono
NCCOSC, RDT&E
Code 4221
53560 Hull Street
San Diego, CA 92152-5001

Prepared by:

ARINC Research
4055 Hancock Street
San Diego, CA 92110-5152

Under Contract:

N66001-93-D-0014,
Delivery Order 0020

Distribution authorized to DOD components only; premature dissemination 2/29/96. Other requests shall be referred to Commanding Officer, Naval Command, Control and Ocean Surveillance Center, RDT&E Division, San Diego, CA 92152-5000

EXECUTIVE SUMMARY

Section 1. This report promulgates a plan for demonstrating Joint Maritime Command Information System (JMCIS) on-line service. Specifically, this plan will lead to an initial proof of concept demonstration of JMCIS on-line service by implementing a package of selected on-line service elements between the JMCIS Development Facility at the Naval Command, Control and Ocean Surveillance Center (NCCOSC) Research, Development, Test & Evaluation Division (NRaD) and a JMCIS site ashore (Commander-in-Chief, U. S. Pacific Fleet (CINCPACFLT) and selected Pacific Fleet ships.

Section 2. The objectives of JMCIS on-line services are:

- Improved JMCIS functionality, performance, reliability
- Easier JMCIS operation & maintenance
- Reduced JMCIS life cycle cost
- Focusable C4I for the warrior

Potential benefactors of on-line services include individual JMCIS shore sites/ships, the overall JMCIS community, and warfighters assigned a collection of JMCIS equipped units.

Within the context of on-line service objectives, potential benefits of on-line services are listed and potential metrics are suggested. Special emphasis is placed on the utility of on-line services to forces afloat.

Section 3. Two service elements (remote system configuration sensing and remote software installation) are selected for use in this demonstration. These service elements have been tested and validated within the laboratory environment. The expected benefits from providing these specific services on-line are discussed.

Section 4. The connectivity requirements for providing on-line services are reviewed. These connectivities have been previously demonstrated in an on-line services context (although no services have as yet been provided).

Section 5. A phased implementation approach is defined as follows:

On-line services between work stations in a lab (internal communications)
On-line services between work stations in a lab (external communications)
On-line services between lab and shore site (CINCPACFLT)
On-line services between lab and selected Pacific Fleet ships.

Implementation issues and milestones are presented.

Section 6. Recommendations are made for the formation of a working group to implement the on-line services demonstration.

TABLE OF CONTENTS

APPENDICES

LIST OF TABLES

LIST OF FIGURES

THIS PAGE

INTENTIONALLY

LEFT BLANK

SECTION 1
INTRODUCTION

1.1 REPORT OBJECTIVE

The purpose of this report is to promulgate a plan for demonstrating Joint Maritime Command Information System (JMCIS) on-line service. Specifically, this plan will lead to initial proof of concept demonstration of JMCIS on-line service by implementing a package of selected on-line service elements at a JMCIS site ashore (CINCPACFLT) and selected Pacific Fleet ship(s).

1.2 BACKGROUND

JMCIS consists of two elements: JMCIS-Afloat, which developed out of the Naval Tactical Command System-Afloat (NTCS-A), and JMCIS-Ashore, which developed out of the Operations Support System (OSS). It is engineered by NRaD and sponsored by the U. S. Space and Naval Warfare Systems Command (SPAWAR). Because of the long history of support by NRaD for OSS and the relatively recent change in the system to become JMCIS-Ashore, the term OSS is still commonly used to refer to laboratories, software segments and tools used in support of JMCIS-Ashore. JMCIS sites ashore have been established at major command centers for CINCPAC and CINCPACFLT in Hawaii, the Naval Command Center (NCC) in Washington, D. C., CINCUSACOM and CINCLANTFLT in Norfolk, CINCUSNAVEUR in London, NAVELEXCENDET in Naples, and CTF 72 in Kama Seya. In addition, JMCIS has been/will be installed on selected ships. (A listing of acronyms is provided as Appendix A.)

JMCIS is produced and operated in an evolutionary development environment. As a result, JMCIS is constantly undergoing changes. These changes are installed on geographically diverse operational systems serving operational and administrative commanders on a nearly continuous basis. These changes have required associated services (such as configuration management, software installation, and testing) on the part of the JMCIS development community. Traditionally, these services have been provided at the JMCIS site, ashore and afloat.

This report deals with expanding the JMCIS service concept to include services provided on-line between the JMCIS Development Facility at NRaD and the JMCIS site, ashore and afloat. This service concept is introduced in Section 2.

Special emphasis is placed on defining the benefits to be derived from on-line service.

An initial proof of concept demonstration will be conducted. This demonstration will provide selected service elements (described in Section 3) on-line (over connectivity described in Section 4) to CINCPACFLT and selected Pacific Fleet ship(s).

Implementation issues are reviewed in Section 5.

1.3 SCOPE

The principal focus of this report is the implementation of a plan for demonstrating JMCIS on-line support (over the JMCIS WAN). The initial demonstration focuses on a selected package of service elements (remote systems configuration and remote software installation). This service package will be provided on-line in a laboratory environment, to a JMCIS shore site (CINCPACFLT), and to selected Pacific Fleet ship(s).

An objective of this plan is to demonstrate the benefit of such on-line services, both in the context of the selected service package and also in terms of scaleable enhancements to the service package as the service package is expanded to meet the needs of each JMCIS site/ship.

As we progress through initial demonstration of proof of concept, to generic on-line service packages, to service packages tailored for individual ships and shore sites, the scope of future versions of this report will be expanded to provide a more comprehensive description of on-line services and the manner in which they are defined, connected, provided, operated, and maintained.

1.4 TERMINOLOGY

Key terms used in this report are introduced below.

a. JMCIS Services. Services provided to JMCIS users. These services include installation of upgrades, planned and corrective maintenance, testing, and other activities associated with the employment of an operational system. Traditionally, these services are provided on the JMCIS site/ship.

b. JMCIS On-line Services (OLSs). Services provided to a JMCIS site through on-line connectivity. This connectivity need not be continuous. Indeed, control and security considerations may result in JMCIS shore site/ship control of when connectivity is established. Additionally, for ships, communications considerations may drive the scheduling of on-line service sessions. Representative on-line services are discussed in “JMCIS Wide Area Network Report, 30 September 1995” (Reference 1 in Appendix B, Bibliography) in terms of potential support and operational (day-to-day operation of the JMCIS system) service elements.

c. JMCIS Service WAN (JSWAN). The wide area network that provides on-line service connectivity between the JMCIS Development Facility at NRaD and various JMCIS sites, ashore and afloat. Currently, this connectivity is provided by NCCOSC Command Internet (NCI Net) from NRaD to CINCPACFLT and SIPRNET access at CINCPACFLT to other JMCIS sites. It is anticipated that the physical connectivity comprising the JSWAN may change as on-line service matures in terms of service elements and customers served.

c. On-Line Service Session. A period of time during which the JMCIS site/ship is connected to the JMCIS WAN for the purpose of receiving JMCIS on-line service.

d. Support Service Elements. Service elements associated with the principal on-line support areas, currently defined as configuration management, software distribution & installation, and testing. Representative support service elements are listed in Table 1-1. These elements are discussed in more detail in Reference 1 (see Appendix B).

e. Operational Service Elements. Service elements associated with the day-to-day operation of the JMCIS system at the JMCIS site. These service elements are focused on the operation of the site network (LAN or MAN) that interfaces and interoperates with the JMCIS Service WAN during on-line service sessions. During such sessions, operational service elements include traditional communication and network management functions. Outside of on-line service sessions, operational service elements are focused on the functions associated with the operation and maintenance of JMCIS. In essence, operational service elements help manage communications and networks during on-line service sessions and help operate and maintain JMCIS, regardless of whether or not such a session is taking place. Representative operational service elements are listed in Table 1-2. These elements are discussed in more detail in Reference 1 (see Appendix B).

f. JMCIS Suite. The organized collection of resources performing JMCIS functions at a shore site/on board ship. This collection may include work stations, networks, and other facilities. In the context of on-line services, it may include work stations dedicated to managing the on-line service session, work stations that manage software installations, and work stations that can be segregated from the operational portion of JMCIS to test JMCIS software before installation.

Table 1-1
Representative Support Service Elements

Support Service Elements	
Configuration Management	· Planning · Control · Current Configuration (Snapshot) · Relational Configuration History · Configuration Compatibility · Resource Allocation · Configuration Modifications
Software Distribution & Installation	· Planning · Control · Distribution · Pre Installation Test & Check Out (PITCO) · Installation · Configuration Management Updates
Testing	· Planning · Control · Installation Concurrent Testing · Post Installation Testing · Troubleshooting · Traditional · Collaborative · Performance Metrics · Certification

Table 1-2
Representative Operational Service Elements

Operational Service Elements	
JMCIS WAN Management	· Management Applications · Initiate Management Tasks · Collect Management Information · Agents · SunNet Manager Agent · Proxy Agent
Operator Training & Certification	· Prebriefing · Walk Through · Post Briefing · Training · Certification
Transaction Audits & Analyses	· Transition Tracking · Routine · Targeted · Browsing Audit Machines · Trend Analyses
Resource Allocation Support	· Resource Status · Planned Changes · What-If Analyses · Allocation Promulgation
Life Cycle Cost Accounting	· Resource Costs · Transaction Costs · Cost Benefit Analyses · What-If Analyses · Running Tallies
Security	· Communications Security · Physical Security · Information Warfare Protect

1.5 REPORT STRUCTURE

In addition to this introductory section, this report is structured as follows:

Section 2 provides a concept of operations for on-line services. Emphasis is placed on the utility of such services to individual JMCIS ships and sites, to the JMCIS community as a whole, and to the warfighter supported by one or more JMCIS suites.

Section 3 describes the service elements (remote system configuration sensing and remote software installation) that are included in the demonstration service package. Remote software installation involves a relatively minor patch rather than a major upgrade.

Section 4 describes the connectivity requirements for demonstrating on-line services.

Section 5 describes our implementation approach.

SECTION 2
CONCEPT OF OPERATIONS

2.1 ON-LINE SERVICE OBJECTIVE

The objectives of JMCIS on-line service (OLS) are:

- Improved JMCIS functionality, performance, reliability
- Easier JMCIS operation & maintenance (O&M)
- Reduced JMCIS life cycle cost
- Focusable C4I for the warrior

2.2 SERVICE CONCEPT

On-line service (OLS) is defined in terms of individual service elements. Representative service elements are described in Reference 1. Service elements are divided into two classes:

- Support service elements (see Table 1-1) are elements associated with the principal on-line support, currently defined as configuration management, software distribution & installation, and testing.

- Operational service elements (see Table 1-2) are elements associated with the day-to-day operation of the JMCIS system at the JMCIS site/ship. These service elements are focused on the operation of the site network that interfaces with the JMCIS Service WAN (JSWAN) during on-line service sessions. During such sessions, operational service elements include traditional communication and network management functions. Outside of on-line service sessions, operational service elements are focused with the operation and maintenance (O&M) of JMCIS at the site/ship. This O&M focus includes analyzing past on-line service sessions and planning for an on-going series of on-line service sessions.

Service elements are combined into service packages. The demonstration service package consists of the following service elements:

- Remote System Configuration Sensing
- Remote Software Installation (Patch)

2.3 FUTURE SERVICES

As JMCIS service elements are defined and validated, they will be combined into generic service packages (ashore & afloat). Generic service packages will be tailored for each site/ship receiving on-line service.

Initially, on-line service sessions will involve the exchange of services (and associated information) between the JMCIS Development Facility at NRaD and the serviced site/ship. This is the construct for on-line services for this report.

Eventually, this exchange of services and information may be expanded to provide for a more robust and synergistic level of service. Potential service providers and receivers in an on-line service session are listed in Table 2-1.

Table 2-1
Potential Service Providers and Receivers
in an On-line Service Session

Provider	Receiver
On-line service relationship for this report	
NRaD	Individual Shore Site/Ship
Possible future on-line service relationships	
NRaD	Regional Mirror Sites
CINC	CINC
CINC	CINC Assets
CJTF	JTF
Commander CVBF	CVBF
CATF	ATF
Peer	Peer

To successfully demonstrate the concept of on-line JMCIS software services, a relationship must exist between NRaD and at least one shore site and between NRaD and at least one ship. Demonstration services to be provided through this relationship are discussed in Section 3. After the concept is proven through demonstration of the limited services described in this document, significant additional capabilities can be established. Those additional capabilities require additional relationships. Note the first possible future on-line service relationship listed in Table 2-1 is between NRaD and Regional Mirror Sites. Mirror Sites are computer host systems that provice a “mirror image” of the information or software available at the primary site. The feasibility and benefit of mirror site establishment for JMCIS software distribution is discussed at the end of Section 3.

2.4 CONNECTIVITY CONCEPT

On-line connectivity is provided over the JMCIS Service Wide Area Network (JSWAN). Currently, this connectivity is provided by NCCOSC Command Internet (NCI Net) from NRaD to CINCPACFLT and SIPRNET access at CINCPACFLT to other JMCIS sites. Plans have been approved and equipment ordered to connect NRaD to CINCLANTFLT via NCI Net as well.

A general design principal is to access SIPRNET via non tactical circuits whenever possible in order to minimize the tactical impact of on-line service.

It is anticipated that the physical connectivity comprising the JSWAN may change as on-line service matures in terms of service elements and customers served.

Demonstration connectivity is discussed in Section 4,

2.5 IMPLEMENTATION CONCEPT

The implementation concept for our demonstration consists of:

- In Section 3...a package of service elements that have been previously employed between connected work stations within a laboratory environment.

- In Section 4...connectivity between NRaD and JMCIS site/ship(s) that has been previously demonstrated in an on-line services context.

- In Section 5...an implementation approach that builds on existing networking initiatives and sequences through the following phases:

    1. Work stations within an NRaD laboratory environment (interior communications)
    2. Work stations within an NRaD laboratory environment (exterior communications)
    3. NRaD to shore site
    4. NRaD to ship(s).

2.6 ON-LINE SERVICE ISSUES

The provision of on-line services to an operational JMCIS site/ship raises several issues regarding control, security, scheduling, training, and operational continuity. The plan described in Section 5 (and frameworked in Appendix E) will address these issues in a manner that is tailored to the concerns of the individual site/ship(s) involved in the demonstration.

The following discussion, of a more general nature, provides background information for individuals developing the test plan.

At CINCPACFLT, there is a JMCIS Beta Test Site, physically and logically separated from the operational JMCIS suite. This test site is used to test software installations prior to the official cut-over of the overall JMCIS suite to a new version. This Beta Test Site can be employed to address some of the issues mentioned above.

On-line support to a ship is a complex matter. A ship (and embarked staff) has multiple, competing demands placed on its resources. On many occasions, these demands may simply preclude the scheduling and execution of an on-line service session. Two items particularly drive the utility (high or low) of on-line services to the afloat unit. These items are C4I operational tempo (optempo) and connectivity. Examples of operationally oriented states of C4I optempo and connectivity that may drive the utility of on-line services (OLS) are presented in Table 2-2.

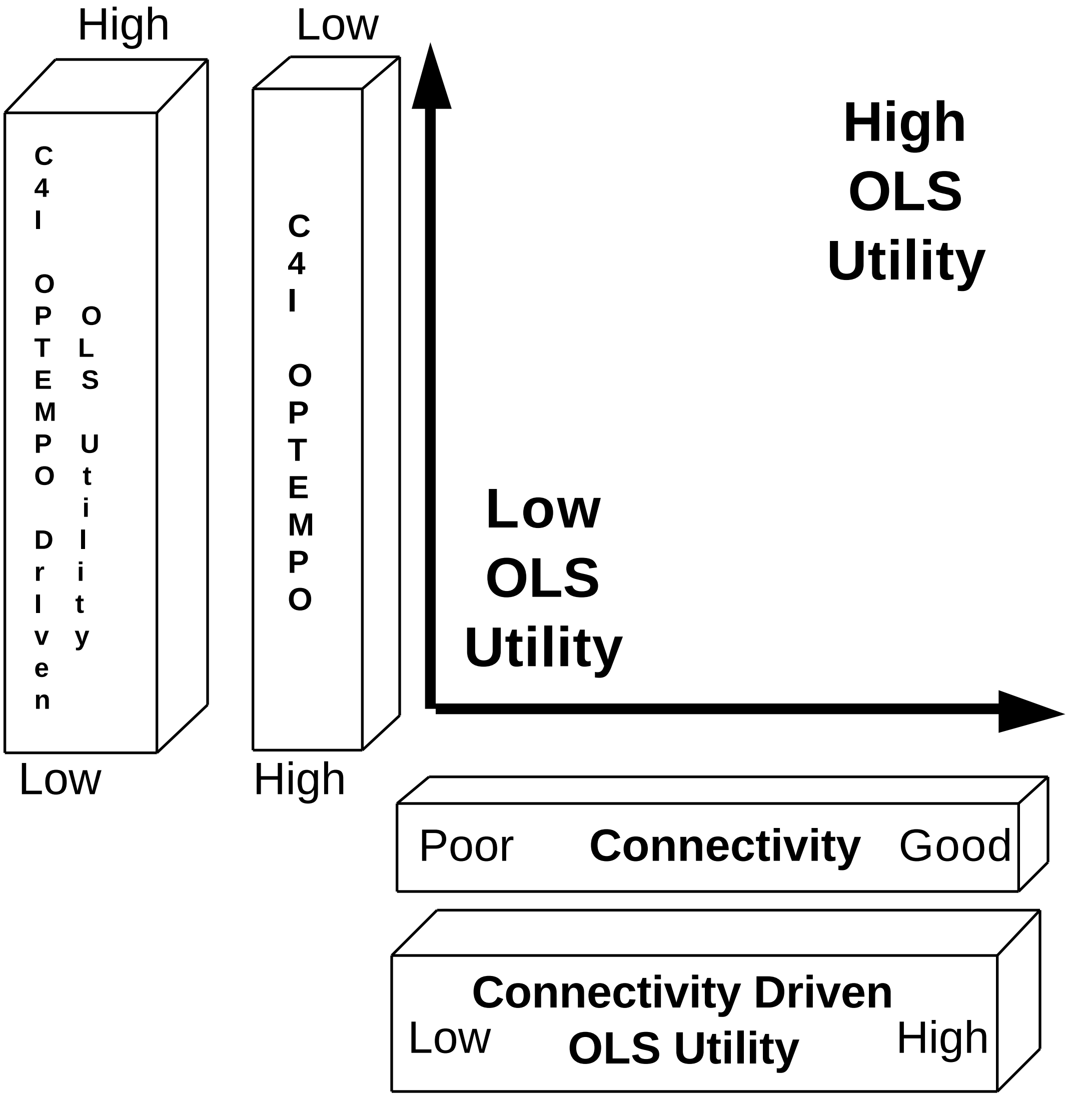
Table 2-2
On-line Service Utility Drivers
for Afloat Units

	At Sea	In Port
C4I Optempo (Low Optempo) [High OLS Utility] (High Optempo) [Low OLS Utility]	· Stand Down · ISE · Routine Fleet Ops · Exercises · Contingency Ops · Hostilities	· Stand Down · Maintenance Availability · RADHAZ/HERO/EMI Restrictions · In Port Exercises · Training · Rehearsals · Simulation · Demos · Testing · Collaborative Planning · Inspections · In Port Operations · Harbor Security · Guard Ship · Heavy Weather Watch · C4I Ready Ship · Pre Sortie Preps
Connectivity (Good Connectivity) [High OLS Utility] (Poor Connectivity) [Low OLS Utility]	· Fully Reliable & Available, Band Width Adequate, Duplex (FRABWAD) Comms · Reliability & Availability Restrictions · Band Width Restrictions · Some Duplex Restrictions · Some Comms Outages · Ship LPI Comms with BG Hub · Ship in Minimize · Complete Ship Comms EMCON · Complete Ship Comms Outage	· Hard Wired FRABWAD Comms · RF FRABWAD Comms · Reliability & Availability Restrictions · Band Width Restrictions · Some Duplex Restrictions · Some Comms Outages · Complete Comms Outages

In general... the lower the C4I optempo, the higher the utility...the better the connectivity, the higher the utility. Obviously there are exceptions to this generalized rule; but it is helpful to consider circumstances under which on-line services will be most useful. This concept is depicted in Figure 2-1.

Figure 2-1 Generalized On-line Service Utility

CC



In any case, there are circumstances where on-line services can be of utility to forces afloat over a wide range of C4I optempos and connectivity. Representative examples are provided as Service Vignettes in Appendix C (Services).

The utility of on-line services is explored in more detail in Paragraph 2.7 in terms of benefits accrued within the context of on-line service objectives listed in Paragraph 2.1.

2.7 ON-LINE SERVICE BENEFITS

On-line support will generate benefits at multiple levels, including the individual shore site/ship, the JMCIS development and operational community as a whole, and the warfighter (such as a Joint Task Force Commander) who directs a collection of JMCIS equipped units in pursuit of a focused mission.

The objectives of JMCIS on-line service, introduced in Paragraph 2.1, are repeated here for ease of reference:

- Improved JMCIS functionality, performance, reliability (“ilities”)
- Easier JMCIS operation & maintenance (O&M)
- Reduced JMCIS life cycle cost
- Focusable C4I for the warrior (C4IFTW)

Table 2-3 suggests possible objective categories in which each level of user might perceive a benefit from on-line services.

Table 2-3
Potential Benefits from On-line Services

	Individual JMCIS Site/Ship	JMCIS Community	JMCIS Warfighter
Improved “ilities”	·	·	·
Easier O & M	·	·	
Reduced Cost	·	·	
Focusable C4IFTW	·		·

Benefits will be both qualitative and quantitative. Potential metrics include:

Improved Functionality. Getting newer versions earlier.

Improved Performance. Performance against various time and other standards.

Improved Reliability. Traditional reliability metrics (e.g., Mean Time Between Failures) (MTBF) and, perhaps more importantly, Mean Time to Repair (MTTR)). Additional metrics will focus on the ease of testing and troubleshooting, the ability of the commander served by the JMCIS suite to control the troubleshoot and repair effort, and the confidence that commander places in JMCIS short and long term.

Easier O & M. Ease of operation given various states of JMCIS reliability. Ease of identifying system anomalies and transition into various maintenance modes. Accuracy of configuration status and applicability of configuration report formats to O & M related functions. Reduced training and certification requirements. Organizational focus of transaction and audit reports and analyses.

Reduced Cost. Various life cycle costs including travel. Savings from smart COTS purchases, inventory reductions, etc.

Focusable C4I for the Warrior. Ability to focus a collection of JMCIS suites to serve a commander. Ease, speed, and effectiveness of identifying and installing mission related patches. Ease and accuracy of system readiness monitoring and associated system resource allocation decision making. System repair triage decision making (see Service Vignettes in Appendix C).

Benefits to be derived from the proof-of-concept demonstration are discussed in Section 3 (Paragraph 3.4).

SECTION 3
DEMONSTRATION SERVICE

3.1 INTRODUCTION

A large range of potential on-line services are available to JMCIS users as described in “JMCIS Wide Area Network Report”, 30 September 1995 (Reference 1). This implementation plan will demonstrate two services currently available. These services are:

- Remote System Configuration Sensing
- Remote Network Software Installation

These services exist in the form of tools developed by NRaD Code 4221. This code is responsible for development, installation, and support of the OSS segments of JMCIS. The performance of this task requires ongoing testing of new versions, patches, and upgrades of JMCIS software. It also involves extensive direct support in the form of installation, troubleshooting, on-site training, and maintenance of JMCIS software at each of the operational sites running OSS segments of JMCIS. In the course of performing these tasks, Code 4221 personnel identified a need for custom software tools to perform certain tasks.

3.2 REMOTE SYSTEM CONFIGURATION SENSING

.
Installing JMCIS in a wide variety of environments requires the ability to query each individual host system regarding configuration. The System Configuration Sensing (SCS) tool conducts this query and generates a report of actual hardware and software configuration. The SCS tool has been successfully used both in the laboratory (Lab 360) and at operational sites. In the past, NRaD Code 4221 representatives have taken the tool with them to operational sites and used it on-site to query system configuration. Experience in the Lab demonstrates that the tool is also capable of being used remotely to query system configuration.

3.3 REMOTE SOFTWARE INSTALLATION (PATCH)

As part of the testing procedures, JMCIS software needed to be installed on numerous machines connected to a network. In the OSS Laboratory (Lab 360), a self-contained network is established with different logical segments separated by a router and with multiple workstations attached to each segment. Without a remote installation tool, every patch or upgrade installation required the operator to physically carry a tape from one machine to another and manually go through the steps to perform the upgrade at each workstation. Each workstation also needed to have a tape drive attached. Since tape drives are not usually attached to every workstation, a portable tape drive would need to be carried from one workstation to another.

The JMCIS software developer did provide a remote access software tool for JMCIS. The tool is useful, but it does not meet all of Code 4221's needs. The JMCIS remote access tool allows one to access a tape drive physically connected to a remote machine. With this tool, a patch or upgrade on tape could be inserted in one drive, or the data copied to a hard drive. Then the data could be sequentially accessed over the network from each of the workstations where the software needed to be installed. This is a "pull" type tool, where data is "pulled" off a remote drive. This tool does negate the need to physically carry a portable tape drive from one workstation to another, however, the upgrades are still time consuming since the tool still requires the operator to physically move to each workstation and manually go through the procedures at that station to do the upgrade.

To provide the desired added capability, NRaD Code 4221 personnel programmed another tool. The Remote Network Software Installation tool is a "push" type tool. Software patches or upgrades are first copied to the hard drive of a designated server. The server has the tool installed. Using this tool the patch is "pushed" to other workstations on the network. The most important advantage of this tool is that the operator does not need to physically move from one workstation to another to accomplish the upgrade. All machines can be upgraded remotely from the installation server. Equally convenient is the fact that multiple machines can be upgraded in parrallel vice serial installation required by other tools and procedures.

Although originally programmed to meet the need of operators in a self-contained LAN, the Remote Network Software Installation tool is not limited to that environment. The tool can be used to remotely install all sizes of software modules, from small, simple patches to large complex ones. The tool can be resident in the remote "pushing" site, or it can be remotely controlled while resident at the target site. Thus, for small patches, the tool can be used to remotely install a patch on a single workstation. For large patches, network bandwidth considerations may dictate that the patch should be transmitted or physically delivered to the remote site and that the Installation tool then be installed in an on-site server and remotely controlled to install the change to the entire JMCIS operational network.

3.4 ANTICIPATED BENEFITS

The use of both tools described above has significant potential benefit to operational commands running JMCIS. Both tools will save time and make the work of JMCIS technicians much more effective. Significant benefits to operational commands will also result from improved service, more rapid response times, and flexibility.

3.4.1 REMOTE CONFIGURATION SENSING TOOL BENEFITS

The regular and consistent use of the Remote Configuration Sensing Tool will have at least two benefits: it will aid in troubleshooting efforts, and it will save time while producing improved technical support to JMCIS sites.

First, the tool has the potential to be useful in troubleshooting certain system problems. If the tool were used regularly, then records could be kept of system configurations when the machine was running well. If a problem later developed, the tool could be run again to see if configuration changes may have contributed to the problem.

Second, the tool will save technician analysis time, improve preparation for technical support visits and thus provide better technical support. When NRaD personnel travel to operational sites for assist visits, they are not always sure what software and/or hardware is necessary to bring to ensure successful task completion. If the Remote System Configuration Sensing tool could be run to identify exact configuration of each JMCIS machine at the site, they could ensure that all necessary software tools, patches, drivers, and applications as well as appropriate hardware components were shipped and available on-site before they arrive. This would save time and provide much better service to operational customers.

3.4.2 REMOTE NETWORK INSTALLATION TOOL BENEFITS

Like the Remote Configuration Sensing Tool, use of the Remote Network Installation Tool will also save time for both technical support personnel and operators of JMCIS sites. Because installing patches now involves sending a technician out on-site, small patches tend to not be installed as soon as they are available, unless they are critical to system performance. The trend would be to wait for a larger patch or group of patches to install. This consolidation of effort is a logical and prudent means of managing the expense of travel and per diem and also a way to reduce time lost to travel. If a remote software installation tool were available, new patches could easily be installed as soon as they were available for distribution. The process would go faster, because their would be no travel delays; and small changes could be made more often, keeping the system configuration completely up-to-date.

The system could also be made to be much more responsive to changing operational environments. If a JMCIS site in a crisis response situation faced problems with system bugs, or simply needed minor modifications to adapt to the operational environment, these changes could be quickly installed using the Remote Network Installation Tool.

Installation of system upgrades throughout the JMCIS LAN on operational sites could be more easily adapted to the rapidly changing schedules of operational units. NRaD could send tapes containing the upgrades to the operational unit. The operational site support personnel could copy the upgrade files onto a server and install the Remote Network Installation Tool. Then the upgrade could be put on hold until operational schedules allowed sufficient availability to complete the install. Without the problem of coordinating travel schedules and lodging for NRaD technicians to meet the ship, the upgrade could be controlled remotely from NRaD and performed at the convenience of the ship.

3.5 DEMONSTRATION SERVICES SUMMARY

In summary, this plan will provide a demonstration and test of two of the many services available to JMCIS users. The Remote Configuration Sensing Tool and the Remote Network Installation Tool both have potential of providing significant benefits for both support technicians and operational users. Connectivity required for these on-line services is discussed in Section 4. Implementation issues are discussed in Section 5.

3.6 FOLLOW-ON SERVICES - THE NEXT STEP

In addition to the services chosen for this initial demonstration, additional JMCIS On-line services either exist or are in the process of being produced, as documented in Reference 1 (see Appendix B). Plans have already been made to expand services offered to operational users as quickly as possible after successful completion of this demonstration. The most immediate beneficial service currently available is probably the JMCIS On-line Library (JOL). JOL already exists on a microcomputer at NRaD and is accessible to CINCPACFLT and Pacific Fleet connected units via NCINET (this connection is discussed in Section 4). Patches, updates and information files for JMCIS OSS segments are available for download.

The JOL could be made more easily accessible to potential users by establishing mirror sites. Many commercial software vendors and information providers have recognized the value of mirror sites. Mirror Sites are computer host systems that provice a “mirror image” of the information or software available at the primary site. Potential exists for significant bottlenecks to develop when only a single site is available for access and download. This bottleneck can be alleviated by distributing copies of the information or software to be downloaded onto multiple computers at diverse locations. Using multiple computers to manage multiple connections is inherently more efficient than using one computer to manage the same multiple connections. Equally important is the fact that users of the World Wide Web, commonly referred to as “the Web”, can be accessing sites from half way around the world. Although relatively transparent to the user, these long distance Web connections go through multiple smaller networks. Each of these intermediate network connections is referred to as a “hop”. Reducing the “hop count” ,or number of intermediate network connections, can increase connection reliability and improve data transfer performance. Thus by providing mirror sites for information and software download which are closer to the potential users, access is improved and download more efficient.

JOL should be expanded to include all available JMCIS updates and patches and then it should be cloned to distributed mirror sites. Using World Wide Web technology such as Web Browsers, Common Gateway Interfaces (CGI), and Uniform Resource Locator (URL) links, sites could be set up to provide exceptional software response to users. Operational JMCIS users could browse the JOL home page or various mirror sites to find software and information they need and then download and use it. The technology already exists to do this and it is being used widely on the Web. As mentioned above, many software vendors offer downloadable software accessible on the Web. A potential user logs onto the vendor’s home page and finds the listing for the software he or she wants. The vendor’s home page then allows the user to choose the source location of the download from a list of mirror sites that hold the software and then download it using the same Web Browser used to view the home page. Most current Web pages offering this service require the user to either know or guess about network architecture to ensure most efficient download site choice.

The JMCIS mirror sites for JOL should offer advice on the download home page that tells the potential user which mirror site would be best based on his current location. To offer accurate advice, NRaD needs to study the topology of the networks that will be used for software distribution and determine the best locations for mirror sites. Best locations would be those that provide best network performance and quickest access to potential operational JMCIS users. Memoranda of Agreement will be required with the mirror sites defining service provided and accessibility. The sites may need supplemental equipment such as additional mass storage devices to allow accessible storage of all potential

JOL software as well. This valuable service can and should be vigorously pursued upon successful completion of the initial demonstration test. Milestones and planning for mirror site establishment are beyond the scope of this document but will be the subject of follow-on documentation.

SECTION 4
DEMONSTRATION CONNECTIVITY

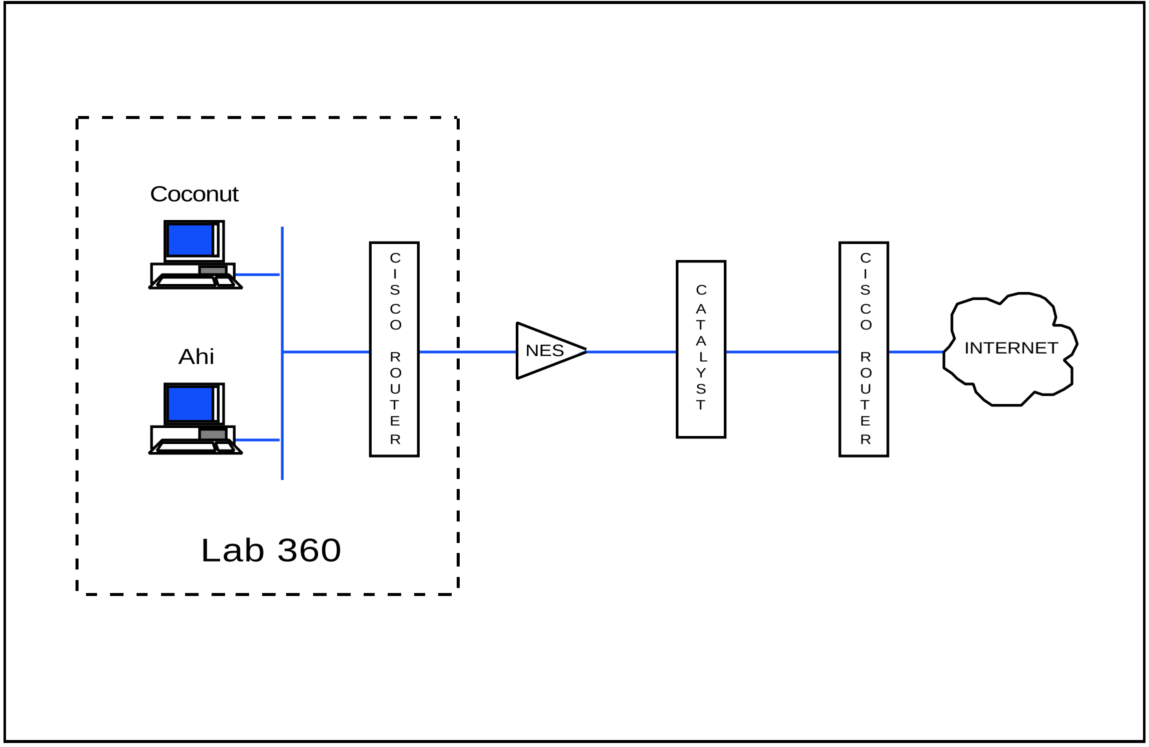
4.1 INTRODUCTION

Connectivity is required between NRaD and the shore site (CINCPACFLT) and selected Pacific Fleet ship(s) receiving the on-line demonstration services discussed in Section 3. One criterion for selecting these services was to avoid the imposition of high bandwidth requirements on this connectivity. This section surveys demonstration connectivity in terms of the JMCIS Service WAN, CINCPACFLT and Selected Pacific Fleet ships. Security is addressed in terms of Memoranda of Agreement (MoA).

4.2 JMCIS SERVICE WAN

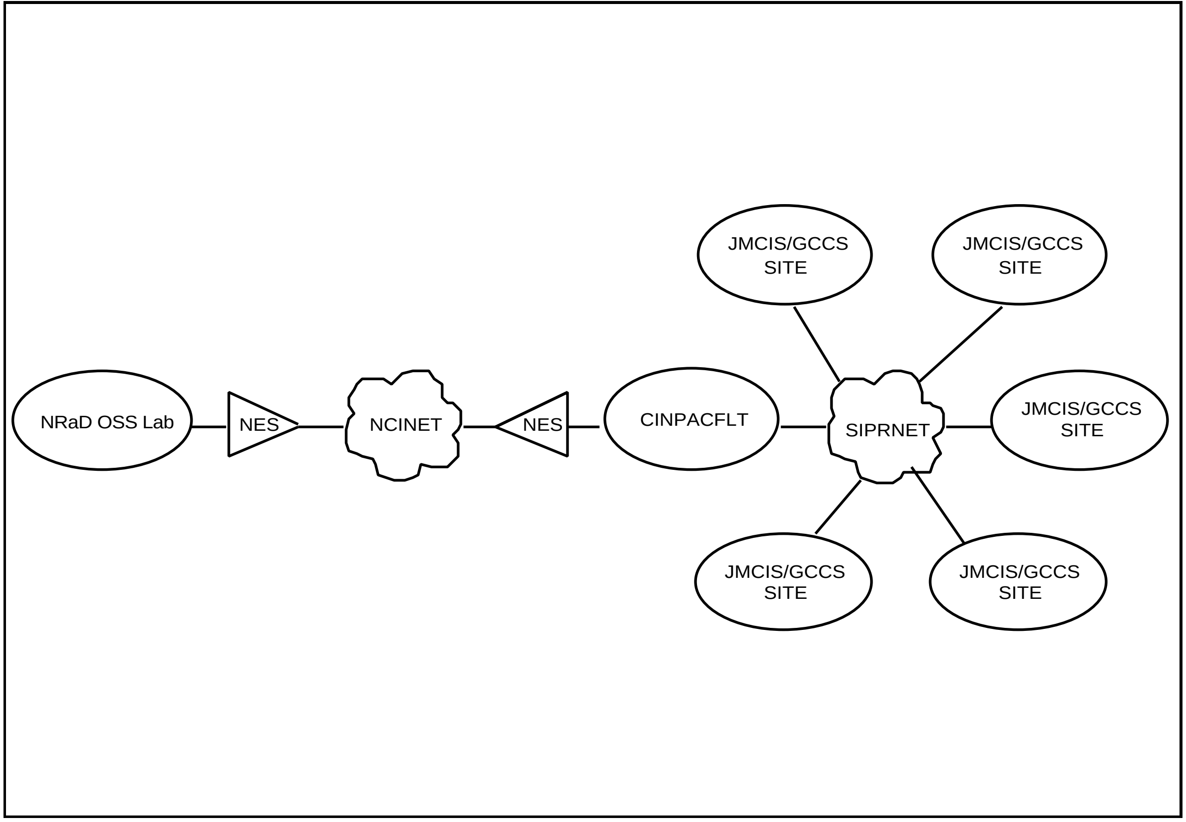
The JMCIS Service WAN originates at the JMCIS Development Facility (OSS Support Lab), Building 600, NRaD. Figure 4-1 depicts the configuration of this facility.

Figure 4-1 JMCIS Development Facility



Currently, the JMCIS Development Facility connects with CINCPACFLT over the NCCOSC Command Internet (NCI Net), as depicted in Figure 4-2. This connectivity provides (physically at CINCPACFLT) access to SIPRNET and, hence, additional JMCIS locations.

Figure 4-2 JMCIS Service WAN (JSWAN)



4.3 FLEET CINC CONNECTIVITY

Connectivity at CINCPACFLT is documented in Reference 1. Equipment has been ordered and a plan approved to establish a similar connection from NRaD to CINCLANTFLT. Consummation of the network connection awaits delivery of a key piece of network equipment and final completion of a Memorandum of Agreement (MOA) between CINCLANT and NRaD. Therefore, by third quarter FY96, NRaD should have full NCI Net connectivity directly to both CINCPACFLT and CINCLANTFLT.

4.4 SELECTED PACIFIC FLEET SHIP(S) CONNECTIVITY

Typically, connectivity with underway afloat units will require, at some point, transmission by radio frequency methods. This involves use of a Standard Tactical Entry Point (STEP), such as a Naval Computer and Telecommunications Area Master Station (NCTAMS). Possible ship-shore connectivity for ships equipped with Motorola Network Encryption Systems (NESs) are documented in Reference 2 (see Appendix B).

4.5 SECURITY

Security issues are addressed in terms of a Memorandum of Agreement (MoA) between NRaD and the command receiving on-line services.

MoAs relevant to this demonstration are as follows.

- CINCPACFLT - NRaD MoA, dated 12 September 1996, (Reference 3 in Appendix B).
- CO Selected Pacific Fleet Ship(s) - NRaD MoA, Reference 4 {not available, Feb 96}.

SECTION 5
IMPLEMENTATION

5.1 INTRODUCTION

This report describes (Section 3) services to be demonstrated and (Section 4) connectivity required to provide those services on-line. This section discusses the implementation of these demonstration on-line services.

5.2 ON-LINE IMPLEMENTATION STATUS

The issue of network connectivity required for this demonstration is essentially solved. The general connections described in Section 4 and the specific NRaD connections described below confirm this fact. In addition, Navy initiatives are in-progress which will assure network connectivity to all potential users of JMCIS on-line services.

5.2.1 GLOBAL NETWORK INITIATIVE

The Global Network Initiative (GNI) is a Navy initiative to provide wide area network connectivity for GCCS and JMCIS. It is a SECRET level IP network which will be a superset of existing nets, will link those nets, and will cover connection “gaps”. Networks to be included are: Secret Internet Protocol Router Network (SIPRNET), Air Force Command and Control Network (AFC2N), Commander in Chief U. S. Pacific Fleet Wide Area Network (CINCWAN), Fleet Commanders Wide Area Network (FLTWAN), Tactical Command and Control System (TCCS), and Navy Command and Control System (NCCS).

Mr. Randy Cieslak, NRaD Code 4204, is the PACFLT JMCIS Site Representative (CINCPACFLT Code N6B1). In that capacity he recently released a memorandum (Reference 5 in Appendix B) giving status of the GNI. Per the Cieslak memorandum, most of the difficult coordination issues, such as domain names, host names, IP addresses, gateway and router management have been solved or nearly so. Essential issues not yet resolved have all been identified and are currently being worked.

GNI will eventually connect almost all JMCIS users in both Atlantic and Pacific Fleets. CINCPACFLT, *USS BLUE RIDGE* (LCC 19), *USS CORONADO* (AGF 11), *USS EISENHOWER* (CVN 69), and most JMCIS shore sites are connected to one or more of these classified IP networks. The GNI has gone a long way toward solving many of the technical, control, addressing, and political questions that have prevented widespread classified IP connection previously. Therefore, if NRaD could obtain a connection to GNI, connectivity would soon be available to all potential users of JMCIS software services.

5.2.2 NRaD CONNECTIVITY

NRaD currently has two different connections to classified networks that provide a link to potential target sites for this demonstration. These connections also provide access to GNI.

As stated in Section 4, the OSS Laboratory, Lab 360, has a direct connection to CINCPACFLT via NCINET. An analogous connection is being established with CINCLANTFLT. The CINCLANTFLT connection is waiting for delivery of key networking equipment now on order (Motorola NES to be delivered in Spring 1996). CINCPACFLT and CINCLANTFLT are connected to SIPRNET. The NCINET connection is now set up so that workstations in NRaD Lab 360 can be connected to SIPRNET using CINCPACFLT routers. This connection has several advantages. First, it is relatively high speed. The data line has between T1 and half T1 capacity. The second advantage of this connection is that for data communication between CINCPACFLT and NRaD it does not compete with tactical or operational network traffic. Contention with operational traffic is only a consideration when using the CINCPACFLT connection to SIPRNET communicating with units beyond CINCPACFLT.

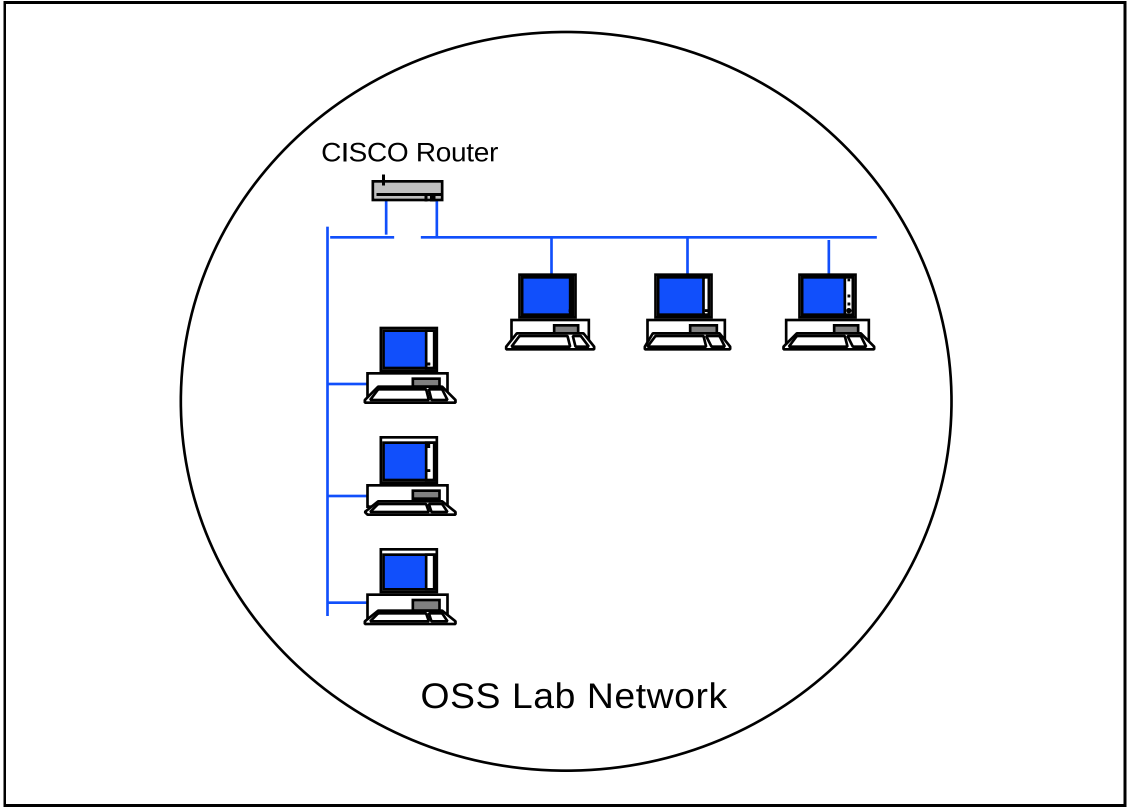
NRaD also has a direct connection to SIPRNET. SIPRNET access is distributed to several sites on the NRaD campus including Lab 350 which is directly next to the OSS Laboratory, Lab 360. There is currently a physical connection between Lab 360 and Lab 350, but there is not logical connectivity from Lab 360 out through the Lab 350 SIPRNET access. Disadvantages of this connection are that it is relatively slow and is shared by numerous NRaD users. The Lab 350 SIPRNET connection is currently a 9600 baud line, but is scheduled to be upgraded to a 384 Kb line in the near future. NRaD Code 80 has established an operational requirement for the higher volume line and will be using a significant portion of that capacity to fulfill operational tasking.

Therefore, Lab 360 can now be connected to target sites via two separate paths. Sufficient bandwidth should be available on the Lab 350 SIPRNET connection to facilitate a small demonstration and test of JMCIS on-line services. For larger demonstrations, or for continued operational use, however, the NCINET connection is preferred.

5.3 PHASED DEMONSTRATION APPROACH

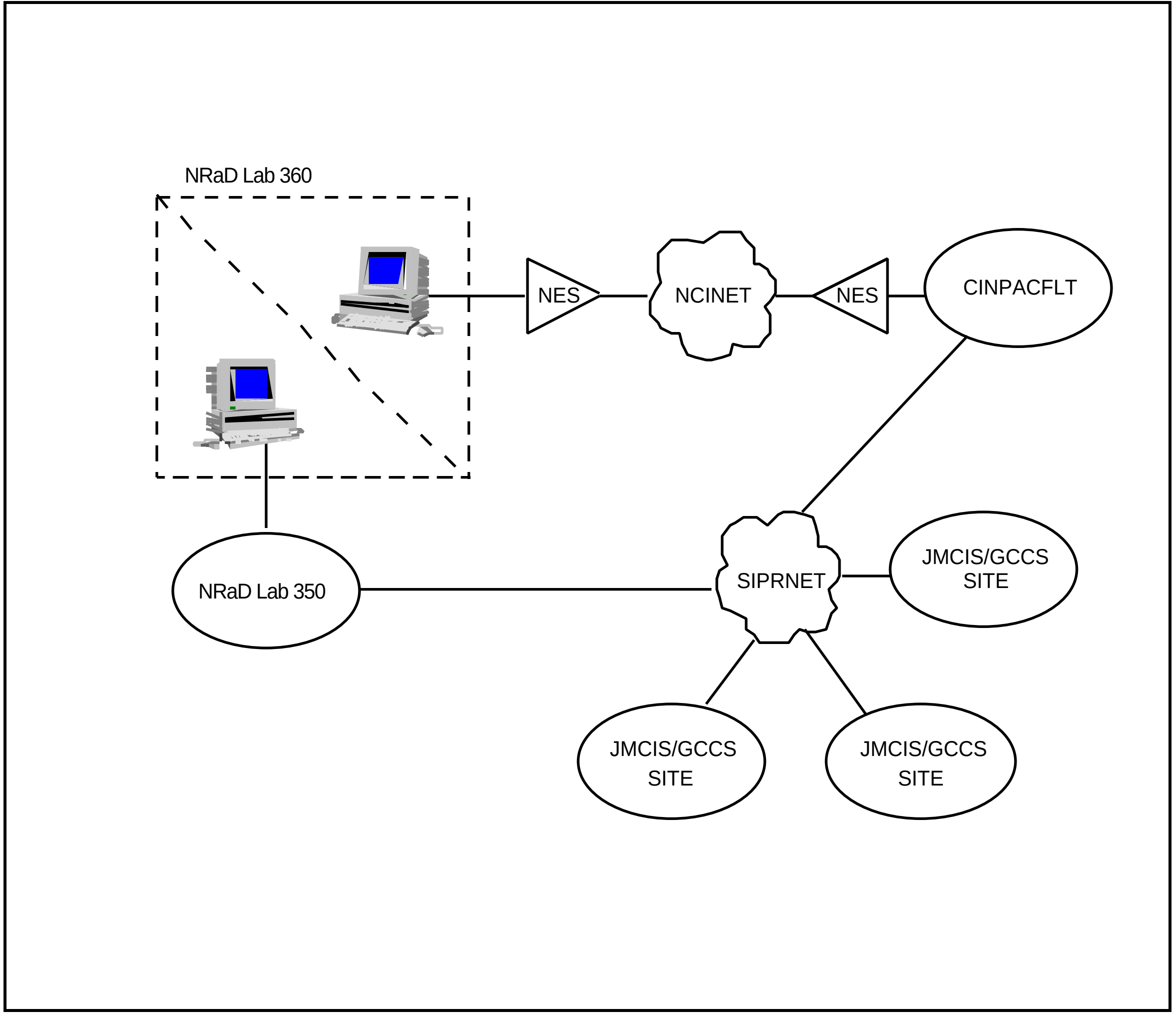
To properly test the limitations and demonstrate the capabilities of the designated tools, the demonstration will proceed in four (4) phases. First the tools should be tested from one network segment to another within a single laboratory. This will allow full testing of capability in a controlled environment without the complexities of external communication and routing. Figure 5-1 depicts the network connectivity that will be used for Phase One of the demonstration and test.

Figure 5-1 Phase One Connectivity.



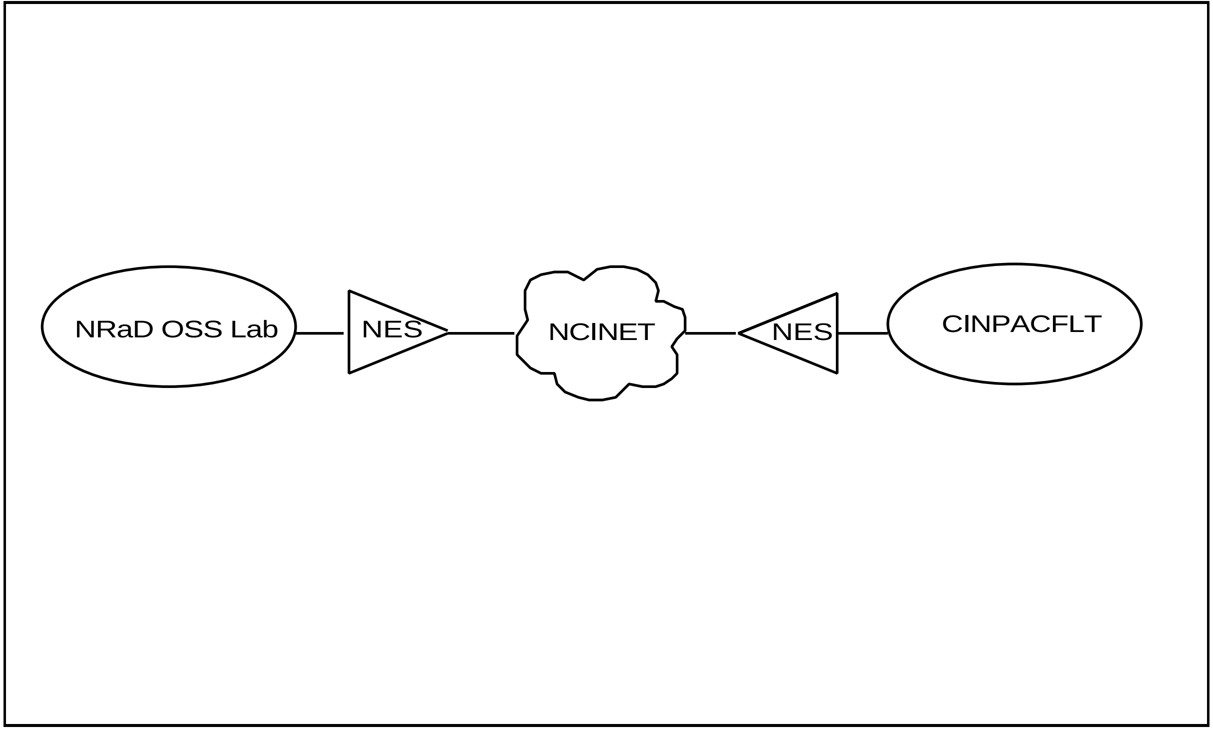
Second, the tools should be tested from a workstation within a laboratory to another workstation in the same, or adjoining laboratory using an external network connection. This adds the complexity of external communication, but still allows direct control of both sides of the transaction by laboratory testing personnel. As described in Section 5.2.2 above, connections now exist which would allow Phase Two to proceed. Figure 5-2 below depicts connectivity to be used for Phase Two.

Figure 5-2 Phase Two Connectivity.



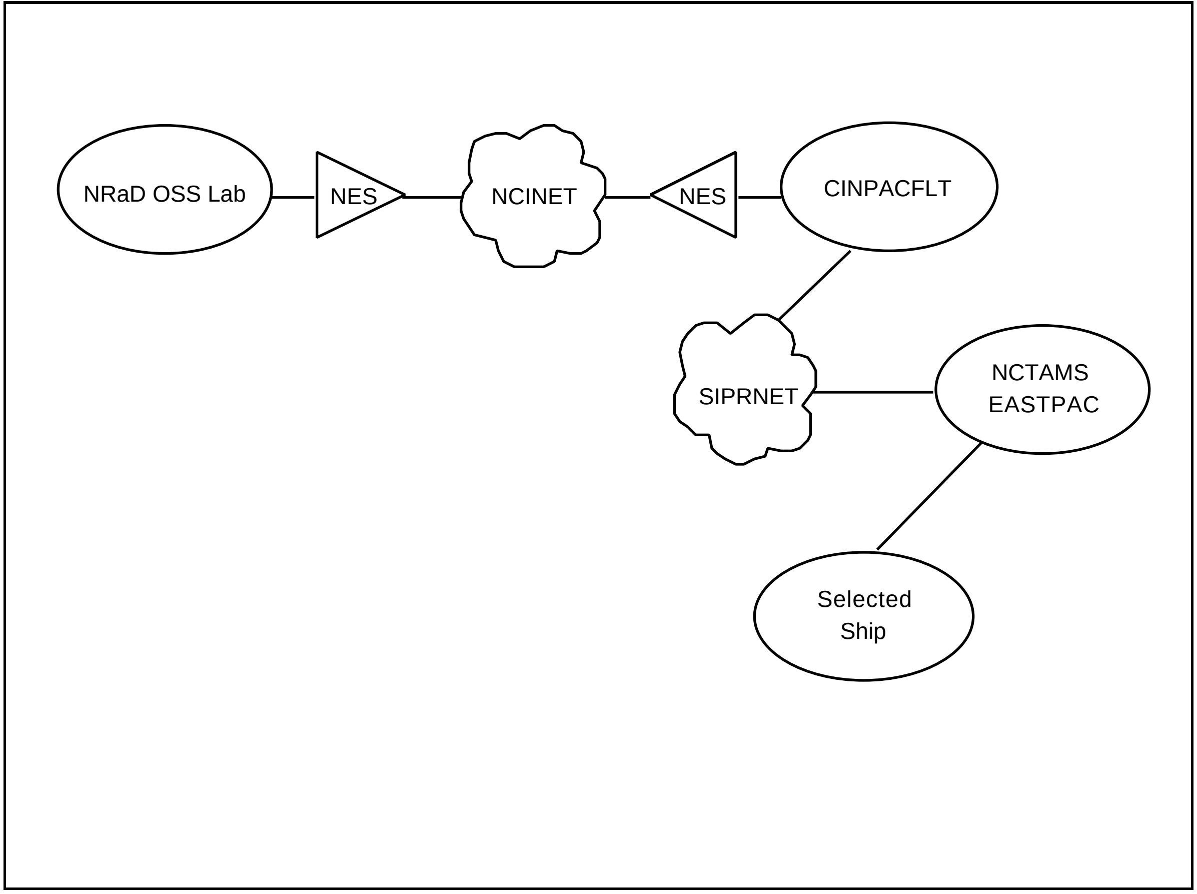
The third phase involves testing while connected to a host system outside NRaD. After the tools have been successfully exercised and procedures refined in the first two phases, the tools will next be tested from an NRaD laboratory to a shore site. This adds the complexity of dealing with an external command, remotely coordinating with on-site personnel, and dealing with a target environment not under the direct physical control of the testers. Connectivity available to facilitate this phase is discussed in Section 4 and Subparagraph 5.2.1 above and is depicted in Figure 5-3.

Figure 5-3 Connectivity to be used for Phase Three.



In the fourth phase, the tools will be tested from the laboratory to a ship. This adds the complexity of dealing with mobile, tactical, operational units and being forced to comply with appropriate procedures to gain permission and access to an operational system. Most important, it also demonstrates the use of the tools in the environment most likely to achieve greatest benefit from their remote use. Figure 5-4 depicts the connectivity to be used for Phase Four of the demonstration test.

Figure 5-4 Phase Four Connectivity.



The planning phases can be summarized as follows:

1. Laboratory to laboratory with internal network connection.
2. Laboratory to laboratory with external network connection.
3. Laboratory to shore JMCIS site.
4. Laboratory to ship JMCIS platform.

5.4 DEMONSTRATION AND TEST PLAN DEVELOPMENT

To facilitate implementation of the demonstration project, a Demonstration Plan Framework is provided as Appendix E to this document. An important prerequisite to initiation of the demonstration is the development of a complete and detailed test plan that will provide both methodology and evaluation criteria to assess the value of the demonstration project.

During the course of normal JMCIS software development and test, all patches and segments are tested in the OSS Software Engineering & Integration Test (SEIT) Facility, NRaD Lab 360G. Within this Lab two separate network segments are available with a router between and JMCIS workstations attached on each segment. Thus, if patches were chosen for this test that have already undergone initial testing at the OSS SEIT Facility, Phase One could be counted as complete and the demonstration could proceed to Phase Two. If Phase Two, Three, or Four results show the need for changes in procedures, software tools, or the patches themselves, then the modifications should be retested starting with Phase One. Therefore, the Demonstration Plan Framework in Appendix E shows all four phases of normal demonstration and test to allow for this potentially iterative process even though the initial demonstration will undoubtedly start at Phase Two.

Tests in the OSS SEIT Facility are conducted by OSS contractor support personnel. To facilitate the testing functions necessary for new JMCIS versions and patches, these contractors have created a set of software test tools tailored to JMCIS. Hereafter, and in Appendix E, these tools will be referred to as the OSS Test Tools. The OSS Test Tools need to be used at each phase of the demonstration in order to adequately assess the value and success of the demonstration. A detailed test plan needs to be generated specifying how the tools will be used in each phase of the demonstration. At the beginning of each phase, the OSS Test Tools should be used to establish system baseline. During and at the end of each phase the tools need to be used again to assess the effects and success of procedures performed.

Although this document is designed to primarily address only the initial demonstration plan, continuous expansion and improvement of JMCIS On-line Services is the ultimate goal. As services are expanded the OSS Test Tools will continue to be modified and enhanced as well. As the tools mature, regression testing procedures should be added to future test plans. The initial demonstration will not include rigorous regression testing because the limited nature of initial service demonstration does not require it, but anticipated future services will be extensive enough to indicate the need for regression testing.

In addition to production of the test plan, a number of important issues need to be addressed before the demonstration plan can be completed in detail and implemented. Critical implementation issues and suggested implementation milestones are surveyed in paragraph 5.5.

5.5 IMPLEMENTATION ISSUES

For the demonstration plan to successfully proceed, a number of issues must be resolved. Some critical issues are already resolved or essentially complete.

Others will need to be addressed in both the detailed test plan and milestones. A partial list of important implementation issues follows.

- Selection of demonstration patches. Although the two demonstration services have been selected, specific JMCIS patches to be used have not. Since numerous patches exist which suit the needs of the test, this task may seem trivial. However, selection of patches will affects several other planning factors. First, the size of the patch selected will affect network bandwidth requirements. Second, the particular patch or patches selected will affect different JMCIS terminals. Selection of the patch for demonstration, then, must be made with the particular target sites in mind and consideration given to specific hardware and software configuration present at the target site.

- Connectivity. Reliable network connectivity will need to be established and maintained with each anticipated target site. This involves both physical connection and logical connection, such as Domain Name Service and IP address assignment, as appropriate. As stated above, the issue of physical connectivity seems to be mostly solved, but not all permissions and logical connections are complete to allow all phases of the demonstration to continue. To establish and maintain a reliable connection will require continued management of the connectivity issue.

- Site selection, especially ship selection.

- Is a MoA required? Depending on sites chosen and extent of the demonstration, a Memorandum of Agreement defining network security concerns may be required.

- If a MoA is required by the target ship, who will the parties to the MOA? Can agreement be reached directly with the ship, or will the embarked staff need to be involved as well?

- Timing of the demonstration (when to test). Operational schedules may have significant impact on demonstration timing.

- Root privileges. Both the Remote Configuration Sensing tool and the Remote Network Software Installation tool require root access to the target JMCIS workstation. NRaD Code 4221 personnel have evaluated modifying the tools to use less than root access, but the nature of the tasks performed and constraints of UNIX based computer systems requires root access for the tools to be successful. For instance, the Remote Configuration Sensing Tool needs to determine hard disk usage. Hard disk status and performance are only accessible to a user with root privileges in a UNIX system. Likewise, the Remote Software Installation Tool may require root access to successfully install a new patch. Depending on the nature of the patch being installed, certain processes may need to be shut down either because those processes interfere with the install, or because they may damage the system or make it unstable when run concurrently with the patch installation. In order to kill running processes initiated by another user in a UNIX system requires root privileges. Thus root permissions are a necessity to use these tools.

- What to test. A steering group needs to be formed to define critical test plan elements. At a minimum, the following capabilities should be tested:
    1. How do the tools and networks perform with various sized patches?
    2. Can an update of a single workstation be performed remotely from Lab 360G?
    3. Can several workstations at a remote site be updated with initiation and control of the update being performed from Lab 360G?
    4. What happens if connectivity is lost or interrupted during the update?

- Evaluation criteria. What factors should be used to judge the demonstration's success?

- Generation of a detailed test plan. A complete plan must be created describing specific test procedures, how the OSS Test Tools will be used, what will be assessed, and how the evaluation criteria will be applied. The test plan needs to allow for establishment of initial system baseline, in process testing, and after action evaluation of the system to determine what has been affected by the software upgrade or fix.

- On-site evaluation. After the patch or upgrade installation is complete, assistance will be required to evaluate the effects of the upgrade. Therefore, on-site personnel will need to be involved in after action testing, evaluation, and reporting back results.

5.6 IMPLEMENTATION MILESTONES

A partial list of implementation milestones is provided as Table 5-1.

Table 5-1
Implementation Milestones

		Fiscal Year					
		95	96				97
Milestone	Status	Q4	Q1	Q2	Q3	Q4	Q1
Define Representative On-line Service Elements	Complete	.					
Establish JSWAN Connectivity with CINCPACFLT	Complete	.					
Establish JSWAN Connectivity to SIPRNET	Complete	.					
Demonstrate JSWAN Connectivity to Forces Afloat	Complete		.				
Complete MOA for CINCPACFLT On-line Services	Complete	.					
ID Demo Players				.			
Form Demo Working Group				.			
Specify Demo Service Package				.			
Define CINCPACFLT Demo Configuration				.			
Define JMCIS Afloat Demo Configuration					.		
Promulgate Demo Test Plan					.		
Complete MOA for JMCIS Afloat On-line Services					.		
Phase 1 (Lab/IntCom) Demo	Complete		.				
Phase 2 (Lab/ExCom) Demo				.			
Phase 3 (CINCPACFLT) Demo					.		
Phase 4 (Afloat) Demo						.	
Promulgate Demo Lessons Learned						.	
Promulgate Scaled (Based on Demo) On-Line Services Benefits Analysis						.	
Promulgate On-line Services Full Implementation Road Map							.

.

THIS PAGE

INTENTIONALLY

LEFT BLANK

SECTION 6
CONCLUSION

6.1 SUMMARY

This report presents an implementation plan for demonstrating JMCIS on-line services at CINCPACFLT and selected Pacific Fleet ship(s).

Potential benefits of providing on-line services throughout the JMCIS community are discussed.

Two service elements (Remote System Configuration Sensing, and Remote Network Software Installation) are selected for the demonstration. These service elements must be specified in more detailed terms relative to the shore site/ship(s) that will participate in the demonstration.

Connectivity requirements for the demonstration can be accommodated using existing NCI Net and SIPRNET connections. Other connectivity options are also feasible.

A phased implementation plan is established involving:

On-line services between work stations in a lab (internal communications)
On-line services between work stations in a lab (external communications)
On-line services between lab and shore site (CINCPACFLT)
On-line services between lab and selected Pacific Fleet ships.

Implementation issues and milestones are presented.

6.2 RECOMMENDATIONS

It is recommended that a working group be formed to implement the on-line service demonstration. Special emphasis should be placed on:

- The identification and accomplishment of implementation milestones.

- The identification, resolution and documentation of associated implementation issues.

THIS PAGE

INTENTIONALLY

LEFT BLANK

.

APPENDIX A
ACRONYMS

AFC2N	Air Force Command & Control Network
ARG	Amphibious Ready Group
ATF	Amphibious Task Force
BG	Battle Group
C^{4}I	Command, Control, Communications, Computers, & Intelligence
C^{4}IFTW	C^{4}I for the Warrior
CGI	Common Gateway Interface
CINCLANTFLT	Commander-in-Chief, U. S. Atlantic Fleet
CINCPAC	Commander-in-Chief, U. S. Pacific Command
CINCPACFLT	Commander-in-Chief, U. S. Pacific Fleet
CINCUSACOM	Commander-in-Chief, U. S. Atlantic Command
CINCWAN	CINCPACFLT Wide Area Network
CJTF	Commander Joint Task Force
COMNAVFOR	Commander, Naval Force (Country)
COMPATWING	Commander, Patrol Wing
COMPHIBGRU	Commander Amphibious Group
COMSEVENTHFLT	Commander, U. S. SEVENTH Fleet
COMSUBGRU	Commander, Submarine Group
COMTHIRDFLT	Commander, U. S. THIRD Fleet
CONOPS	Concept of Operations
COTS	Commercial of the Shelf
CTF	Commander Task Force
CVBG	Carrier Battle Group
EASTPAC	Eastern Pacific
EMCON	Emission Control
FLTWAN	(Numbered) Fleet Commanders' Wide Area Network
FRABWAD	Fully Reliable & Available, Band Width Adequate Duplex (Communications)
GCCS	Global Command and Control System
GNI	Global Network Initiative
IP	Internet Protocol
ISE	Independent Steaming
JFACC	Joint Force Air Component Commander
JMCIS	Joint Maritime Command Information System
JOL	JMCIS On-line Library
JOSDEP	JMCIS On-line Services Demonstration Plan
JSWAN	JMCIS Service Wide Area Network
JTF	Joint Task Force
LAN	Local Area Network

LPI	Limited Probability of Intercept
MAN	Metropolitan Area Network
MoA	Memorandum of Agreement
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAVELEXCENDET	Naval Electronics System Center Detachment
NCC	Naval Command Center
NCCOSC	Naval Command, Control and Information System
NCCS	Navy Command & Control System
NCINET	NCCOSC Command Internet
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCTS-A	Navy Tactical Command System - Afloat
NES	Network Encryption System
NRaD	NCCOSC Research, Development, Test & Evaluation Division
O&M	Operations & Maintenance
OLS	On-line Services
OPTEMPO	Operational Tempo
OSS	Operations Support System
PITCO	Pre Installation Test & Check Out
POCs	Points of Contact
RF	Radio Frequency
ROK	Republic of Korea
SCS	System Configuration Sensing
SEIT	System Engineering & Integration Test (Facility)
SIPRNET	Secret Internet Protocol Router Network
STEP	Standard Tactical Entry Point
TCCS	Tactical Command & Control System
URL	Uniform Resource Locator
WAN	Wide Area Network
WESTPAC	Western Pacific
www	World Wide Web

APPENDIX B
BIBLIOGRAPHY

1. JMCIS Wide Area Network Report, 30 September 1995

2. IP Addressing Study...Navy Afloat Use of the Motorola Network Encryption System, 1 November 1995

3. Memorandum of Agreement (MoA) between CINCPACFLT and NRaD, dated 12 September 1995

4. Memorandum of Agreement (MoA) between COM{3rd or 7th)FLT, CO USS {selected ship}, and NRaD, {Not available, Feb 96}.

5. “Global Network Initiative (GNI) Status Report” memo, 3 February 1996, R. Cieslak, PACFLT JMCIS Site Representative (Code N6B1)

THIS PAGE

INTENTIONALLY

LEFT BLANK

APPENDIX C
SERVICES

Service Vignettes

Vignette A. In the 90 day period prior to deployment, a carrier battle group (CVBG) had a C4I upgrade availability. During this period, a major new JMCIS version was installed (in port) in each JMCIS equipped ship. The installation seemed to go well and post-installation (pre deployment) testing indicated a successful install. Three days after deploying from San Diego, the battle group starts to experience JMCIS difficulties. Due to the potential serious nature of these problems, bandwidth is allocated for a dedicated period of JMCIS on-line collaborative trouble-shooting. Troubleshooting and associated on-line patches restore JMCIS performance to acceptable levels before the CVBG reaches Pearl Harbor.

Vignette B. Mid-way through a deployment, a CVBG and an Amphibious Ready Group (ARG) are assigned to a Joint Task Force (JTF) for contingency operations. The Commander Joint Task Force (CJTF) embarks on board the CV and the Joint Force Air Component Commander (JFACC) embarks aboard the LHD. The JMCIS performance of the overall JTF is marginal, presumably because of the high C4I optempo imposed on the JTF. A Battle Group Systems Team is made available to the CJTF to help restore JMCIS performance on individual ships. But the CJTF needs assistance in deciding which JMCIS platforms need the team’s services and in which order these services will be provided. There is, in essence, a need for a JMCIS repair triage process and the measure of effectiveness involves how the JTF JMCIS community serves the JTF and the JFACC, not necessarily how an individual JMCIS suite on a particular ship functions. JMCIS on-line services, within the JTF and between the JTF and NRaD aid in this triage process.

Vignette C. Hostilities are rapidly escalating between warring factions in a region of the world vital to United States interests. A new JTF is quickly formed and a CVBG and ARG assigned to the JTF for contingency operations in the region. The JFACC embarks aboard the CV and the CJTF embarks in a dedicated command and control ship. All key task force elements are running JMCIS and it is performing exactly as advertised. However, many elements of this particular contingency operation involve unforeseen tactical situations and potential scenarios. JMCIS in its current configuration is not optimized to meet the needs of this particular operation. A call for help is sent to NRaD asking for JMCIS software modifications to meet this urgent, real-world need. NRaD embarks on a crash development effort and quickly produces a set of JMCIS software patches to add the requested capabilities. Because of the urgency of the situation, the patches are transmitted via SIPRNET to the deployed units. The patches are then installed in all appropriate JMCIS workstations on each ship using remote installation tools. Upgrade of JMCIS systems on deployed units is successfully completed in a very short time to meet the urgent real-world requirements of deployed staffs.

Vignette D. Towards the end of a deployment, a ship is getting ready for a major JMCIS install that is scheduled for after the ship returns to home port. The last time the ship made a post deployment JMCIS install, there were several problems primarily because of a loss of configuration control of the many changes made over the course of the pre deployment work up and the deployment itself. Presently, the ship is in EMCON and unable to get on-line with NRaD. However, using tools installed on board to aid in the process of on-line support, the ship is able to review her JMCIS configuration locally and identify a possible configuration problem. Later, when EMCON is lifted, the ship gets on-line with NRaD and NRaD performs remote system configuration sensing. This information, along with the ship's self assessment, aids in the pre install planning process and contributes to a successful install.

APPENDIX D
POTENTIAL USERS OF SERVICES

1. Potential users capable of receiving services now:

CINCPACFLT
COMPATWING ONE
COMSEVENTHFLT
USS COWPENS (CG 63)
USS BLUE RIDGE (LCC 19)
USS KITTY HAWK (CV 63)

2. Potential users able to receive services within the year (pending planned connections and upgrades):

CINCLANTFLT
COMNAVFOR JAPAN
COMNAVFOR KOREA, CHINHAE ROK
COMNAVFOR KOREA, YONGSONG ROK
COMPHIBGRU ONE
COMSUBGRU SEVEN
USS BELLEAU WOOD (LHA 3)
USS CORONADO (AGF 11)
USS EISENHOWER (CVN 69)
USS INDEPENDENCE (CV 62)

THIS PAGE

INTENTIONALLY

LEFT BLANK

APPENDIX E
TEST PLAN FRAMEWORK

I. PHASE ONE

Phase One: Lab to Lab Using Internal Connection

Phase one is comprised of testing performance of the Remote Configuration Sensing Tool and the Remote Network Installation Tool within the confines of a single Laboratory. To have an effective test, at least two logical network segments should be established with a router between segments. Both tools should be exercised from a workstation on one segment to a remote workstation on another segment. This phase will be conducted within the OSS SEIT Facility, NRaD Lab 360G. JMCIS-Ashore software segments are routinely tested in the OSS SEIT Facility by OSS contractor support personnel. To facilitate the testing functions necessary for new JMCIS versions and patches, these contractors have created a set of software test tools tailored to JMCIS. These tools will be used as part of all phases of this test plan to establish baseline performance and to evaluate success of each phase of the test. Hereafter, these tools will be referred to as the OSS Test Tools.

Phase One Prerequisites

Before Phase One can begin, the following must be decided or performed:

1. Choose JMCIS patch(es) to test.
2. Determine desired results and evaluation factors.
3. Generate a test plan detailing procedures and tools that will be used and expected results for Phase One.

Phase One Conduct of Test

A. Baseline Scan. Conduct a baseline scan of target JMCIS system using the OSS Test Tools. This baseline will be used for comparison with a scan after installation of patch is complete.

B. Test of Remote Configuration Sensing Tool. Run the Remote Configuration Sensing Tool via the router connection to query each potential target workstation.

C. Test of small, single patch remotely installed.

   1. Load a selected patch onto one workstation using the Remote Network Installation tool.

2. Verify successful installation of the single patch on single workstation.
3. Repeat installation of a single patch but purposely interrupt the install in progress to test how the Remote Network Installation tool handles the error. This interrupted can be performed on a second workstation or the original patch can be de-installed and reinstalled on the same workstation in this step. Which procedure will be used should be determined prior to step C performance.
4. Verify results on interrupted installation.

D. Test of large patch installed on several workstations on remote network.
1. Load the Remote Network Installation tool onto a simulated remote server.
2. Copy a large patch onto the hard drive of a simulated remote server.
3. While remotely controlling the Network Installation Tool, install the patch on more than one workstation on the remote network segment.
4. Verify results of remotely controlled installation.

Phase One Evaluation Factors

1. OSS Test Tools will be run again on completion of the patch installations and results will be compared with the baseline scan run prior to test.
2. Direct analysis of the target workstation will be compared with the results of the Remote Configuration Sensing Tool to determine its accuracy.
3. After the remote installation of a small patch, the target workstation will be thoroughly tested using the detailed test plan prepared before this phase.
4. Results of the installation interruption will be evaluated to determine if this technique will be included in Phase Two testing.
5. After remotely controlled installation of the large upgrade on several workstations, each will be thoroughly tested by appropriate operators and technicians using the detailed test plan prepared before this phase.
6. Resulting level of accuracy for all tests will be compared with predetermined performance requirements to decide if the patch and tool may be used in Phase Two as is, or if either will need to be modified. If modification is required, those portions of Phase One affected by the modifications must be retested with satisfactory results before proceeding to Phase Two.

II. PHASE TWO

Phase Two: Lab to Lab Using External Connection

Phase Two will test both the Remote Configuration Sensing Tool and the Remote Network Installation Tool using a network connection external to the OSS SEIT Facility, NRaD Lab 360G. Within Lab 360G two JMCIS network segments will be configured so they are physically and logically separate. Each segment will have one or more JMCIS workstations attached. One segment will connect to SIPRNET via NCINET and the CINCPACFLT SIPRNET connection. The other segment will connect to SIPRNET via Lab 350. This connection scheme is depicted in Figure 5-2. IP is an inherently efficient protocol and will automatically seek the shortest and most efficient route for a designated connection. Therefore, it is very important that both physical cabling and logical addressing be made to ensure that an air gap exists between the workstations within Lab 360 and that the only path to connect them is via external SIPRNET.

Four major areas will be tested in Phase Two:

1. Ability to successfully sense configuration of a workstation using the Remote Configuration Sensing tool over an external network connection.
2. Ability to install a small patch remotely using an external network connection.
3. Performance of the Remote Network Installation Tool when connectivity is interrupted during the install.
4. Ability to remotely control the installation of a large upgrade onto several workstations attached to a remote site LAN.

Phase Two Prerequisites

Before Phase two can begin, the following must be decided or performed:

1. Choose JMCIS patches to use for the demonstration.
2. Establish logical connection to Lab 350 and out to SIPRNET. “Logical connection” includes resolving security concerns and completing any documentation or agreements necessary to establish the connection. Ensure the connection maintains an air gap within Lab 360 separating the workstations attached to NCINET and the workstations connected via Lab 350 to SIPRNET.
3. Desired results and acceptable level of performance for the demonstration tools must be determined prior to the test in order to have a benchmark for evaluation of results. The same performance criteria and evaluation factors should be used for Phases Two, Three and Four.

4. Generate a test plan detailing procedures and tools that will be used and expected results for Phases Two, Three and Four. It is important to devise a test plan and test procedures prior to Phase Two that will be used in all subsequent phases to ensure consistency and accuracy of results.

Phase Two Conduct of Test

A. Baseline Scan. Conduct a baseline scan of target JMCIS system using the OSS Test Tools. This baseline will be used for comparison with a scan after installation of patch is complete.

B. Test of Remote Configuration Sensing Tool. Run the Remote Configuration Sensing Tool via the external connection to query each potential target workstation.

C. Test of small, single patch remotely installed.
   1. Load a selected patch onto one workstation via the external connection using the Remote Network Installation tool.
   2. Verify successful installation of the single patch on single workstation.
   3. Repeat installation of a single patch but purposely interrupt the install in progress to test how the Remote Network Installation tool handles the error.
   4. Verify results on interrupted installation.

D. Test of large patch installed on several workstations on remote network. This will simulate the situation where tapes are prepositioned at the target site because of the large size of the upgrades. Large patches or upgrades could be sent on tape, downloaded from mirror sites close to the target, or downloaded during off-peak network times. The large patch would be copied to a hard disk on the target network and actual installation would be controlled remotely from NRaD. For Phase Two test, the large patch will be loaded on the target network using tape and target network installation will be controlled using the Remote Network Installation tool via the external SIPRNET connection.
   1. Load the Remote Network Installation tool via the external connection onto a simulated remote server.
   2. Copy a large patch onto the hard drive of a simulated remote server.
   3. While remotely controlling the Network Installation Tool, install the patch on more than one workstation on the remote network segment.
   4. Verify results of remotely controlled installation.

Phase Two Evaluation Factors

1. OSS Test Tools will be run again on completion of the patch installations and results will be compared with the baseline scan run prior to test.
2. Direct analysis of the target workstation will be compared with the results of the Remote Configuration Sensing Tool to determine its accuracy.
3. After the remote installation of a small patch, the target workstation will be thoroughly tested using the detailed test plan prepared before this phase and the installed patch will be validated against expected results documented in patch release notes.
4. Results of the installation interruption will be evaluated to determine if this technique will be included in Phase Three testing.
5. After remotely controlled installation of the large patch installation on several workstations, each will be thoroughly tested by appropriate operators and technicians using the detailed test plan prepared before this phase.
6. Resulting level of accuracy for all tests will be compared with predetermined performance requirements to decide if the patches and tools may be used in Phase Three as is, or if either will need to be modified. If modifications are required, those portions of Phases One and Two affected by the modifications must be retested with satisfactory results before proceeding to Phase Three.

III. PHASE THREE

Phase Three: Lab to JMCIS Shore Site

Phase Three will involve conducting the same tests as Phase Two using a remote network connection and a JMCIS Shore Site as target. CINCPACFLT will be the selected shore site because of the excellent connection available through NCINET, and the fact that a MoA already exists between NRaD and CINCPACFLT. The areas to be tested will be the same as in Phase Two except for any modifications resulting from Phase Two evaluation.

As a reasonable precaution, an NRaD representative or team will travel to CINCPACFLT for the initial demonstration of JMCIS On-line Services to observe and assist as necessary with the test. Once the concept of service and appropriate procedures are demonstrated and proven effective, it will not be necessary for NRaD personnel to be on-site.

Phase Three Prerequisites

Before Phase Three can proceed, the following must be provided:

1. CINCPACFLT must designate test workstations. CINCPACFLT has two LAN segments separated by a router for their JMCIS operation. One is informally called the “Beta LAN” segment because it is used to install and test new configurations. After new patches are successfully tested on the Beta LAN they are installed on the operational segment of the CINCPACFLT JMCIS LAN. The workstations designated for this test will probably be on the Beta LAN.
2. CINCPACFLT must set up an account giving NRaD personnel root privileges on the designated machine. Section 5.5 discussed the reasons for the root access requirement.
3. The selected large patch or upgrade must be delivered to CINCPACFLT by most appropriate means in order to be ready for Conduct of the Test.
4. The test plan generated before Phase Two should be reviewed to ensure it is complete and ready to use for evaluation of demonstration test results.

Phase Three Conduct of Test

A. Baseline Scan. Conduct a baseline scan of target JMCIS system using the OSS Test Tools. This baseline will be used for comparison with a scan after installation of patch is complete.

B. Test of Remote Configuration Sensing Tool. Run the Remote Configuration Sensing Tool from NRaD to query each potential target workstation at CINCPACFLT.

C. Test of small, single patch remotely installed.
   1. From NRaD, load a selected patch onto one workstation at CINCPACFLT using the Remote Network Installation tool.
   2. Verify successful installation of the single patch on single workstation.
   3. Repeat installation of a single patch but purposely interrupt the install in progress to test how the Remote Network Installation tool handles the error. (Depending on results of Phase Two, this step may be modified or deleted.)
   4. Verify results on interrupted installation. (Only if item C.3. is performed.)

D. Test of large patch installed on several workstations on remote network.
   1. From NRaD, load the Remote Network Installation Tool on a server at CINCPACFLT.
   2. CINCPACFLT personnel ensure selected large patch is copied onto the hard drive of the designated CINCPACFLT server.
   3. With NRaD remotely controlling the Network Installation Tool, install the patch on more than one workstation on the CINCPACFLT network.

E. Verify results of remotely controlled installation.

Phase Three Evaluation Factors

Phase Three evaluation will be the same as Phase Two evaluation except that verification, analysis, and test of target workstations will be performed by CINCPACFLT personnel using the NRaD test plan generated prior to Phase Two. Results of the evaluation will be used to determine if any modifications are to be made in test plans before conduct of Phase Four.

1. OSS Test Tools will be run again on completion of the patch installations and results will be compared with the baseline scan run prior to test.
2. Direct analysis of the target workstation will be compared with the results of the Remote Configuration Sensing Tool to determine its accuracy.
3. After the remote installation of a small patch, the target workstation will be thoroughly tested using the detailed test plan prepared before Phase Two and the installed patch will be validated against expected results documented in patch release notes.
4. Results of the installation interruption (if it was performed) will be evaluated to determine if this technique will be included in Phase Four testing.
5. After remotely controlled installation of the large patch installation on several workstations, each will be thoroughly tested by appropriate operators and technicians using the detailed test plan prepared before Phase Two.
6. Resulting level of accuracy for all tests will be compared with predetermined performance requirements to decide if the patches and tools may be used

in Phase Four as is, or if either will need to be modified. If modifications are required, those portions of Phases One, Two, and Three affected by the modifications must be repeated with satisfactory results before proceeding to Phase Three.

IV. PHASE FOUR

Phase Four: Lab to Ship

Phase Four will involve conducting the same tests as Phases Two and Three using a remote network connection and a JMCIS equipped ship as target. The areas to be tested will be the same as in Phases Two and Three except for any modifications resulting from Phase Three evaluation.

There are at least three differences between Phase Three and Phase Four:

1. There is will undoubtedly be no Beta LAN on the target ship. Demonstration tests will have to be conducted on the operational JMCIS LAN.
2. It is unlikely that any specific MoA or prior agreements will be in place directly with the target ship, so notification will have to be given, and/or permission obtained from operational commanders.
3. The ship’s operating schedule will be an issue. Timing of the demonstration will have to be adjusted to accommodate the operational needs of the ship and any embarked staff.

As a reasonable precaution, an NRaD representative or team will travel to the target ship for the initial demonstration of JMCIS On-line Services to observe and assist as necessary with the test. Once the concept of service and appropriate procedures are demonstrated and proven effective, it will not be necessary for NRaD personnel to be on-site.

Phase Four Prerequisites

Before Phase Four can proceed, the following must be accomplished:

1. Any required notification, permissions, or agreements necessary must be completed to allow NRaD access to the target ship’s JMCIS workstations to conduct the demonstration.
2. The target ship must designate test workstations.
3. The target ship must determine appropriate timing for the test.
4. The target ship must set up an account giving NRaD personnel root privileges on the designated machine. Section 5.5 discusses the reasons for the root access requirement.
5. The large patch required for part of the test must be delivered to the target ship by most appropriate means.
6. The test plan generated before Phase Two should be reviewed in light of Phases Two and Three results to ensure it is appropriate for on-site evaluation of demonstration test results.

Phase Four Conduct of Test

A. Baseline Scan. Conduct a baseline scan of target JMCIS system using the OSS Test Tools. This baseline will be used for comparison with a scan after installation of patch is complete.

B. Test of Remote Configuration Sensing Tool. Run the Remote Configuration Sensing Tool from NRaD to query each potential target workstation at the target ship.

C. Test of small, single patch remotely installed.

  1. From NRaD, load a selected patch onto one workstation at the target ship using the Remote Network Installation tool.
  2. Verify successful installation of the single patch on single workstation.
  3. Repeat installation of a single patch but purposely interrupt the install in progress to test how the Remote Network Installation tool handles the error. (Depending on results of Phases Two and Three, this step may be modified or deleted.)
  4. Verify results on interrupted installation. (Only if item C.3. is performed.)

D. Test of large patch installed on several workstations on remote network.

  1. From NRaD, load the Remote Network Installation Tool on a server at the target ship.
  2. Target ship personnel ensure selected large patch is copied onto the hard drive of the designated server.
  3. With NRaD remotely controlling the Network Installation Tool, install the patch on more than one workstation on the target ship JMCIS network.

E. Verify results of remotely controlled installation.

Phase Four Evaluation Factors

Phase Four evaluation will be the same as Phases Two and Three evaluation except that verification, analysis, and test of target workstations will be performed by target ship personnel using the NRaD test plan generated prior to Phase Two

1. OSS Test Tools will be run again on completion of the patch installations and results will be compared with the baseline scan run prior to test.
2. Direct analysis of the target workstation will be compared with the results of the Remote Configuration Sensing Tool to determine its accuracy.
3. After the remote installation of a small patch, the target workstation will be thoroughly tested using the detailed test plan prepared before Phase Two and the installed patch will be validated against expected results documented in patch release notes.
4. Results of the installation interruption (if it was performed) will be evaluated.

5. After remotely controlled installation of the large patch installation on several workstations, each will be thoroughly tested by appropriate operators and technicians using the detailed test plan prepared before Phase Two.
6. Resulting level of accuracy for all tests will be compared with predetermined performance requirements to decide if the patches and tools need to be modified. If modifications are required, those portions of Phases One, Two, Three, and Four affected by the modifications must be repeated with satisfactory results before using or installing tools or patches at other sites.

THIS PAGE

INTENTIONALLY

LEFT BLANK